HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484

ĐỀ TÀI: TÌM HIỂU VỀ MÔ HÌNH/KIẾN TRÚC BẢO MẬT CỦA HỆ ĐIỀU HÀNH WINDOWS 11

Các sinh viên thực hiện :

B22DCAT241	Phạm Thị Lệ Quyên
B22DCAT228	Nguyễn Công Việt Quang
B22DCAT242	Nguyễn Đình Quyền
B22DCAT247	Nguyễn Thanh Sơn
B22DCAT248	Nguyễn Thanh Sơn
B22DCAT253	Đinh Thị Thanh Tâm

Tên nhóm: 07

Tên lớp: 01

Giảng viên hướng dẫn: PGS.TS. Hoàng Xuân Dậu

HÀ NỘI 3-2025

PHÂN CÔNG NHIỆM VỤ NHÓM THỰC HIỆN

TT	Công việc / Nhiệm vụ	SV thực hiện	Thời hạn hoàn thành
1	Kiến trúc bảo mật của Windows 11	Nguyễn Công Việt Quang	22/2/2024
2	Đặc tính bảo mật Windows 11	Phạm Thị Lệ Quyên	20/2/2024
3	Demo và đánh giá	Nguyễn Đình Quyền	08/03/2024
4	Các thành phần của hệ thống bảo mật trong Windows 11	Nguyễn Thanh Sơn 247	20/2/2024
5		Nguyễn Thanh Sơn 248	20/2/2024
6	Các công cụ đảm bảo an toàn	Đinh Thị Thanh Tâm	22/2/2024

NHÓM THỰC HIỆN TỰ ĐÁNH GIÁ

TT	SV thực hiện	Thái độ tham gia	Mức hoàn thành CV	Kỹ năng giao tiếp	Kỹ năng hợp tác	Kỹ năng lãnh đạo
1	Nguyễn Công Việt Quang	4	4	3	4	–
2	Phạm Thị Lệ Quyên	5	4	4	4	4
3	Nguyễn Đình Quyền	4	4	4	4	–
4	Nguyễn Thanh Sơn 247	4	4	3	4	–
5	Nguyễn Thanh Sơn 248	4	4	3	4	–
6	Đinh Thị Thanh Tâm	4	4	4	4	–

Ghi chú:

- Thái độ tham gia: Đánh giá điểm thái độ tham gia công việc chung của nhóm (từ 0: không tham gia, đến 5: chủ động, tích cực).
- Mức hoàn thành CV: Đánh giá điểm mức độ hoàn thành công việc được giao (từ 0: không hoàn thành, đến 5: hoàn thành xuất sắc).

- Kỹ năng giao tiếp: Đánh giá điểm khả năng tương tác, giao tiếp trong nhóm (từ 0: không hoặc giao tiếp rất yếu, đến 5: giao tiếp xuất sắc).
- Kỹ năng hợp tác: Đánh giá điểm khả năng hợp tác, hỗ trợ lẫn nhau, giải quyết mâu thuẫn, xung đột
- Kỹ năng lãnh đạo: Đánh giá điểm khả năng lãnh đạo (từ 0: không có khả năng lãnh đạo, đến 5: có khả năng lãnh đạo tốt, tổ chức và điều phối công việc trong nhóm hiệu quả).

MỤC LỤC

MỤC LỤC 4
DANH MỤC CÁC HÌNH VẼ 6
DANH MỤC CÁC TỪ VIẾT TẮT 7
MỞ ĐẦU 8
CHƯƠNG 1. TỔNG QUAN VỀ BẢO MẬT WINDOWS 11 9
1.1 Giới thiệu về hệ điều hành Windows 11 9
1.1.1 Lịch sử và bối cảnh ra đời 9
1.1.2 Những cải tiến hỗ trợ người dùng 9
1.2 Mối đe dọa và giải pháp bảo mật của Windows 11 9
1.2.1 Các mối đe dọa an ninh mạng 9
1.2.2 Giải pháp bảo mật của Windows 11 10
1.3 Kết chương 10
CHƯƠNG 2. KIẾN TRÚC BẢO MẬT CỦA WINDOWS 11 11
2.1 Khái quát 11
2.2 Các mô hình kiến trúc bảo mật 11
2.2.1 Bảo mật Chip-to-Cloud 11
2.2.2 Mô hình Zero Trust 12
2.2.3 Mô hình phòng thủ theo chiều sâu (Defense-in-Depth) 13
2.3 Kết chương 13
CHƯƠNG 3. ĐẶC TÍNH BẢO MẬT CỦA WINDOWS 11 14
3.1 Khái quát 14
3.2 Các đặc tính bảo mật riêng biệt 14
3.2.1 Security by Design & Security by Default 14
3.2.2 Bảo mật ngay từ phần cứng & firmware 14
3.2.3 Loại bỏ mật khẩu truyền thống, tăng cường bảo vệ danh tính 14
3.2.4 Bảo vệ hệ điều hành bằng công nghệ ảo hóa & kiểm soát mã độc kernel 15
3.2.5 Phòng chống tấn công mạng và phần mềm độc hại theo thời gian thực 15
3.3 Kết chương 15
CHƯƠNG 4. CÁC THÀNH PHẦN CỦA HỆ THỐNG BẢO MẬT 16
4.1 Bảo mật phần cứng (Hardware Security) 16
4.1.1 TPM 2.0 (Trusted Platform Module 2.0) 16
4.1.2 Microsoft Pluton 16
4.1.3 Virtualization-Based Security (VBS) 17

4.2 Bảo mật hệ điều hành (Operating System security) 18
4.2.1 Mã hóa và bảo vệ dữ liệu (Encryption and data protection) 18
4.2.2 Bảo mật hệ thống (System security) 19
4.2.3 Bảo mật mạng (Network security) 19
4.2.4 Ngăn chặn virus và các mối đe dọa (Virus and threat protection) 20
4.3 Bảo mật ứng dụng (Application security) 21
4.3.1 Smart App Control 21
4.3.2 Windows Sandbox 21
4.4 Bảo mật danh tính và xác thực (Identity & Authentication Security) 22
4.4.1 Windows Hello 22
4.4.2 Credential Guard 22
4.5 Kết chương 23
CHƯƠNG 5. CÁC CÔNG CỤ ĐẢM BẢO AN TOÀN 24
5.1 Công Cụ Bảo Mật Tích Hợp 24
5.1.1 Windows Security 24
5.1.2 Windows Hello 24
5.1.3 BitLocker 25
5.2 Công Cụ Bảo Mật Nâng Cao 25
5.2.1 Microsoft Defender for Endpoint 25
5.2.2 Virtualization-based Security (VBS) & Hypervisor-Protected Code Integrity (HVCI) 25
5.2.3 Windows Sandbox 26
5.3 Kết chương 26
CHƯƠNG 6. DEMO & ĐÁNH GIÁ 27
6.1 Mô tả mô hình demo 27
6.1.1 Mục tiêu 27
6.1.2 Cấu hình hệ thống thử nghiệm 27
6.1.3 Kịch bản: Kiểm tra bảo vệ thời gian thực (Real-time Protection) 27
6.2 Đánh giá 30
6.3 Kết chương 30
KẾT LUẬN 32
TÀI LIỆU THAM KHẢO 33

DANH MỤC CÁC HÌNH VẼ

Hình 1 - Kiến trúc bảo mật toàn diện Chip-to-Cloud....12
Hình 2 - Mô hình phòng thủ Defense-in-Depth....13
Hình 3 - Con chip TPM....16
Hình 4 - Kiến trúc Microsoft Pluton....17
Hình 5 - Kiến trúc bảo mật dựa trên ảo hóa (VBS)....18
Hình 6 - Yêu cầu khóa khôi phục Bitlocker....19
Hình 7 - Smart App Control chặn tập tin không an toàn....21
Hình 8 - Kiến trúc Windows Sandbox và Host....22
Hình 9 - Cơ chế bảo vệ thông tin đăng nhập với Credential Guard....23
Hình 10 - Windows Security....24
Hình 11 - Windows Hello trên Windows 11....25
Hình 12 - Tiến hành tải file mã độc không thành công do bị chặn bởi SmartScreen....28
Hình 13 – Cố gắng tải file mã độc sau khi tắt SmartScreen....28
Hình 14 - Thông báo của Windows Security khi muốn tải file mã độc....29
Hình 15 - Tắt Real-time protection và thành công tải file mã độc....29
Hình 16 - Windows Security hiển thị thông báo khi phát hiện file mã độc trong máy....30
Hình 17 - Microsoft Defender Antivirus cách ly và tự động xóa file mã độc....30

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
EDR	Endpoint Detection and Response	Phát hiện và phản hồi điểm cuối
FIDO2	Fast Identity Online 2	Tiêu chuẩn xác thực không cần mật khẩu
MFA	Multi-Factor Authentication	Xác thực đa yếu tố
MSA	Microsoft Account	Tài khoản Microsoft
OOBE	Out-of-Box Experience	Quá trình cấu hình ban đầu
TPM	Trusted Platform Module	Mô-đun nền tảng tin cậy
VBS	Virtualization-Based Security	Bảo mật dựa trên ảo hóa
VPN	Virtual Private Network	Mạng riêng ảo
UEFI	Unified Extensible Firmware Interface	Giao diện firmware mở rộng hợp nhất
SMB	Server Message Block	Giao thức chia sẻ tệp

MỞ ĐẦU

Trong bối cảnh công nghệ số phát triển mạnh mẽ, vấn đề bảo mật hệ điều hành ngày càng trở nên quan trọng. Windows 11 – hệ điều hành mới nhất của Microsoft – không chỉ mang đến trải nghiệm người dùng tối ưu mà còn được tích hợp nhiều công nghệ bảo mật tiên tiến. Báo cáo này tập trung nghiên cứu về kiến trúc bảo mật của Windows 11, phân tích các mô hình bảo mật, các thành phần của hệ thống bảo mật cùng với các công cụ và giải pháp bảo mật đi kèm.

Báo cáo bài tập lớn gồm 5 chương với nội dung chính như sau:

Chương 1: Tổng quan về bảo mật Windows 11, bao gồm lịch sử phát triển và các mối đe dọa.

Chương 2: Kiến trúc bảo mật của Windows 11, mô tả các mô hình bảo mật.

Chương 3: Các đặc tính bảo mật của Windows 11.

Chương 4: Các thành phần của hệ thống bảo mật, bao gồm phần cứng, hệ điều hành, ứng dụng, danh tính & xác thực.

Chương 5: Các công cụ đảm bảo an toàn, trong đó có công cụ bảo mật tích hợp và công cụ bảo mật nâng cao.

Chương 6: Demo & đánh giá, bao gồm kiểm tra khả năng bảo vệ thời gian thực của Microsoft Defender Antivirus và giám sát bảo mật qua Windows Security.

CHƯƠNG 1. TỔNG QUAN VỀ BẢO MẬT WINDOWS 11

1.1 Giới thiệu về hệ điều hành Windows 11

1.1.1 Lịch sử và bối cảnh ra đời

Windows 11 được Microsoft công bố vào ngày 24/06/2021 và chính thức phát hành vào ngày 05/10/2021. Đây là phiên bản kế nhiệm của Windows 10, đánh dấu sự chuyển đổi quan trọng trong chiến lược phát triển hệ điều hành của Microsoft.

Những yếu tố dẫn đến sự ra đời của Windows 11 bao gồm:

- Sự thay đổi trong nhu cầu công nghệ: Các công nghệ mới như AI, điện toán đám mây và hybrid work (làm việc kết hợp) đã trở thành tiêu chuẩn, đòi hỏi hệ điều hành linh hoạt hơn.
- Tấn công an ninh mạng gia tăng: Windows 11 được thiết kế với các cơ chế bảo mật mạnh mẽ hơn để đối phó với các mối đe dọa hiện tại.
- Yêu cầu phần cứng mới: Microsoft yêu cầu chạy Windows 11 phải có TPM 2.0, Secure Bôt và bộ xử lý hiện đại để đảm bảo tính bảo mật ngay từ phần cứng.

1.1.2 Những cải tiến hỗ trợ người dùng

Windows 11 mang đến một số cải tiến quan trọng so với Windows 10:

- Hiệu năng tốt hơn:
  - Quản lý bộ nhớ và CPU tốt hơn, giúp tăng tốc độ xử lý.
  - Khởi động nhanh hơn với UEFI Secure Boot và Trusted Boot.
  - Tối ưu hóa điện năng cho laptop và tablet.
- Giao diện hiện đại:
  - Giao diện Fluent Design với các góc bo tròn, hiệu ứng trong suốt và thanh tác vụ (Taskbar) được căn giữa.
  - Snap Layouts và Snap Groups giúp quản lý cửa sổ linh hoạt hơn.
  - Widgets cung cấp thông tin nhanh như thời tiết, tin tức, lịch...
- Tính năng hỗ trợ người dùng:
  - Hỗ trợ ứng dụng Android thông qua Windows Subsystem for Android (WSA).
  - Tích hợp Microsoft Teams vào thanh Taskbar.
  - Hỗ trợ màn hình cảm ứng tốt hơn.

1.2 Mối đe dọa và giải pháp bảo mật của Windows 11

1.2.1 Các mối đe dọa an ninh mạng

Một số mối đe dọa an ninh mạng mà Windows 11 phải đối mặt:

- Tấn công danh tính (Identity Attacks): Hacker sử dụng kỹ thuật phishing, credential stuffing, Pass-the-Hash để đánh cắp thông tin đăng nhập.
- Ransomware: Mã độc mã hóa dữ liệu và yêu cầu tiền chuộc, thường khai thác lỗ hổng Remote Desktop Protocol (RDP) hoặc các phần mềm không cập nhật.
- Tấn công vào chuỗi cung ứng phần mềm (Supply Chain Attacks): Hacker nhắm đến các nhà cung cấp phần mềm để tiêm mã độc vào các bản cập nhật (như vụ SolarWinds).
- Khai thác lỗ hổng phần cứng và firmware: Các tấn công Spectre, Meltdown, Rowhammer có thể khai thác các lỗi vi kiến trúc CPU.

1.2.2 Giải pháp bảo mật của Windows 11

Để đối phó với các mối đe dọa này, Microsoft đã công bố sáng kiến Secure Future Initiative (SFI) vào tháng 11/2023, tập trung vào Secure by Design – Secure by Default (Bảo mật từ thiết kế - Bảo mật theo mặc định). Thế giới đang hướng tới một phương pháp bảo mật theo thiết kế và bảo mật mặc định, nơi các nhà sản xuất công nghệ có nhiệm vụ tích hợp bảo mật ngay từ giai đoạn thiết kế ban đầu, và cung cấp các sản phẩm mang lại bảo vệ ngay khi sử dụng mà không cần cấu hình trước.

Windows 11 cho phép người dùng tập trung vào công việc của mình, không phải cài đặt bảo mật. Các tính năng mặc định như bảo vệ thông tin đăng nhập, tấm chắn phần mềm độc hại và bảo vệ ứng dụng đã dẫn đến sự giảm 62% sự cố bảo mật, bao gồm việc giảm 3 lần các cuộc tấn công vào firmware.

Sự kết hợp giữa phần cứng và phần mềm giúp giảm diện tích tấn công, bảo vệ tính toàn vẹn hệ thống và dữ liệu quan trọng. Các tính năng bảo mật được tích hợp mặc định, bao gồm cách ly ứng dụng Win32, bảo vệ mã thông báo, passkeys và Intune Endpoint Privilege Management, nhằm ngăn chặn các cuộc tấn công. Ngoài ra, Windows Hello và Windows Hello for Business tận dụng TPM 2.0, máy quét sinh trắc học và cảm biến hiện diện để mang lại trải nghiệm đăng nhập an toàn và bảo vệ thông tin người dùng, đồng thời mã hóa BitLocker được tối ưu hóa để tăng cường bảo mật và hiệu suất trên nhiều thiết bị hơn.

1.3 Kết chương

Chương 1 đã cung cấp cái nhìn tổng quan về Windows 11, từ lịch sử phát triển đến những cải tiến quan trọng về hiệu năng, giao diện và bảo mật. Trước những thách thức an ninh mạng ngày càng gia tăng, Windows 11 được thiết kế với các cơ chế bảo vệ mạnh mẽ, giúp tăng cường an toàn cho hệ thống và dữ liệu người dùng. Với sự kết hợp giữa phần cứng và phần mềm, Windows 11 không chỉ mang lại trải nghiệm tối ưu mà còn khẳng định vị thế của một hệ điều hành hiện đại, bảo mật và đáng tin cậy.

CHƯƠNG 2. KIẾN TRÚC BẢO MẬT CỦA WINDOWS 11

2.1 Khái quát

Trong thời đại kỹ thuật số, các mối đe dọa an ninh mạng ngày càng tinh vi và phức tạp. Hệ điều hành Windows 11 được thiết kế với kiến trúc bảo mật đa lớp nhằm bảo vệ dữ liệu, danh tính và thiết bị khỏi các cuộc tấn công mạng. Mô hình bảo mật này không chỉ dựa vào các biện pháp phòng thủ truyền thống mà còn kết hợp các công nghệ hiện đại như ảo hóa, bảo mật phần cứng, trí tuệ nhân tạo (AI) và điện toán đám mây để nâng cao hiệu quả bảo vệ.

Mục tiêu chính của kiến trúc bảo mật Windows 11:

- Bảo mật Chip-to-Cloud (Chip-to-Cloud Security)
- Phòng thủ đa lớp (Defense in Depth)
- Mô hình Không Tin Cậy (Zero Trust Security)

2.2 Các mô hình kiến trúc bảo mật

2.2.1 Bảo mật Chip-to-Cloud

Trên Windows 11, phần cứng và phần mềm phối hợp chặt chẽ để bảo vệ dữ liệu nhạy cảm từ lớp lõi của thiết bị cho đến đám mây. Chip-to-Cloud là mô hình bảo mật từ phần cứng (chip) đến phần mềm và dịch vụ đám mây, đảm bảo mọi tầng của hệ thống đều có cơ chế bảo vệ.

- Lớp bảo mật phần cứng (Hardware Security): Bảo vệ hệ thống từ gốc bằng các công nghệ như mã hóa phần cứng, kiểm soát khởi động an toàn và bảo vệ bộ nhớ, giúp chống lại các cuộc tấn công vào firmware và phần cứng.
- Lớp bảo mật hệ điều hành (OS Security): Sử dụng các cơ chế mã hóa dữ liệu, cô lập tiến trình, bảo vệ bộ nhớ và kiểm soát quyền truy cập, giúp đảm bảo tính toàn vẹn của hệ thống và dữ liệu trước các cuộc tấn công từ phần mềm độc hại.
- Lớp bảo mật ứng dụng (Application Security): Áp dụng các công nghệ cách ly ứng dụng, kiểm soát mã độc và xác thực phần mềm đáng tin cậy, giúp ngăn chặn ứng dụng độc hại xâm nhập vào hệ thống.
- Lớp bảo mật danh tính (Identity Security): Tăng cường xác thực đa yếu tố, đăng nhập không mật khẩu và bảo vệ thông tin đăng nhập, giúp chống lại các cuộc tấn công đánh cắp danh tính và lừa đảo đăng nhập.
- Dịch vụ đám mây (Cloud Services): Cung cấp các công cụ quản lý thiết bị, kiểm soát truy cập và giám sát mối đe dọa trên nền tảng đám mây, giúp bảo vệ dữ liệu và đảm bảo tính liên tục của hoạt động từ xa.
- Nền tảng bảo mật (Security Foundation): Thiết lập các tiêu chuẩn bảo mật trong phát triển phần mềm, chuỗi cung ứng và chứng nhận bảo mật, đảm bảo hệ thống luôn được cập nhật và bảo vệ trước các lỗ hổng bảo mật mới.

Hình 1 - Kiến trúc bảo mật toàn diện Chip-to-Cloud

Mô hình "Chip-to-Cloud Security" được triển khai chủ yếu trên Windows 10 và Windows 11, nhưng hỗ trợ đầy đủ nhất trên Windows 11 với các tính năng bảo mật hiện đại hơn. Windows 11 là hệ điều hành đầu tiên được thiết kế để tận dụng toàn bộ mô hình "Chip-to-Cloud Security", với các yêu cầu phần cứng bảo mật cao hơn như TPM 2.0, VBS, và Secure Boot.

2.2.2 Mô hình Zero Trust

Zero Trust là một kiến trúc và mô hình bảo mật toàn diện đang được triển khai để bảo vệ các hệ thống và dữ liệu trực tuyến. Theo phương châm Zero Trust, không có bất kỳ thiết bị hoặc người dùng nào được tin tưởng mặc định trong mạng, bất kể họ có ở bên trong hay bên ngoài mạng.

Trong kiến trúc Zero Trust, tất cả các yêu cầu truy cập tài nguyên đều được kiểm tra và xác thực, bất kể vị trí hoặc danh tính của người dùng hay thiết bị. Các quyết định truy cập được đưa ra dựa trên nguyên tắc của người dùng, đánh giá danh tính, quyền hạn và ngữ cảnh của việc truy cập. Điều này giúp giảm thiểu rủi ro bảo mật, ngăn chặn các cuộc tấn công từ bên trong mạng và bảo vệ dữ liệu quan trọng khỏi các mối đe dọa.

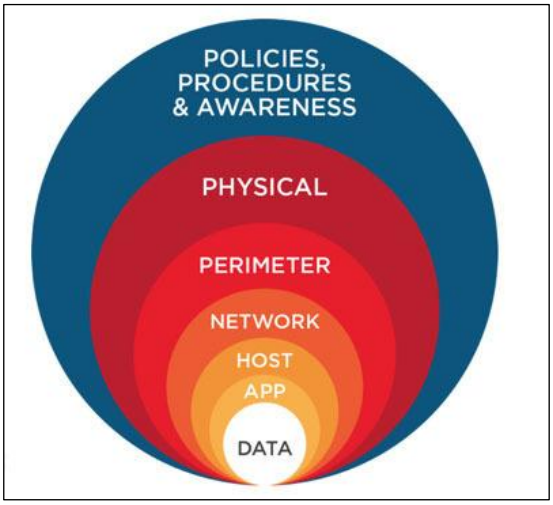
Ba nguyên tắc chính của Zero Trust:

1. Luôn xác thực (Verify Always): Kiểm tra danh tính người dùng, thiết bị và vị trí trước khi cấp quyền.
2. Giới hạn quyền truy cập (Least Privilege): Chỉ cấp quyền cần thiết để tránh rủi ro lây lan khi bị tấn công.
3. Giám sát liên tục (Assume Breach): Mặc định hệ thống có thể bị tấn công, giám sát và phản hồi mối đe dọa theo thời gian thực.

Cách Zero Trust được triển khai trên Windows 11:

- Windows Hello + FIDO2: Giảm thiểu rủi ro tấn công bằng cách thay thế mật khẩu bằng phương thức xác thực an toàn hơn.
- Microsoft Entra ID (Azure AD): Xác thực đa yếu tố (MFA), kiểm tra tình trạng thiết bị trước khi cấp quyền truy cập.
- Conditional Access: Định danh người dùng, ứng dụng và thiết bị trước khi cho phép truy cập tài nguyên quan trọng.

2.2.3 Mô hình phòng thủ theo chiều sâu (Defense-in-Depth)



Hình 2 - Mô hình phòng thủ Defense-in-Depth

Đây là một chiến lược bảo mật sử dụng nhiều lớp bảo vệ để bảo vệ dữ liệu và hệ thống thông tin khỏi các mối đe dọa. Mô hình này dựa trên nguyên tắc rằng không có một lớp bảo vệ nào là hoàn toàn an toàn, do đó, cần nhiều lớp bảo vệ chồng lên nhau.

Windows 11 áp dụng mô hình Defense-in-Depth trong thiết kế bảo mật của hệ điều hành:

- Chính sách, quy trình và nhận thức (Policies, Procedures & Awareness): Microsoft Security Baselines, Windows Defender Security Center.
- Vật lý (Physical): Windows 11 yêu cầu bắt buộc TPM 2.0, Secure Boot...
- Vành đai (Perimeter): Microsoft Defender for Endpoint, Microsoft Entra ID
- Mạng (Network): Windows Defender Firewall, VPN, TLS, DNS Security...
- Máy chủ (Host): Credential Guard & Local Security Authority (LSA) Protection...
- Ứng dụng (App): Smart App Control, Windows Sandbox...
- Dữ liệu (Data): BitLocker, Personal Data Encryption, Email Encryption...

2.3 Kết chương

Chương này đã trình bày ba mô hình bảo mật chính của Windows 11: Chip-to-Cloud, Zero Trust, và Defense-in-Depth. Sự kết hợp của các mô hình này giúp bảo vệ hệ thống toàn diện từ phần cứng đến phần mềm và giúp Windows 11 nâng cao khả năng bảo vệ trước các mối đe dọa an ninh mạng hiện đại.

CHƯƠNG 3. ĐẶC TÍNH BẢO MẬT CỦA WINDOWS 11

3.1 Khái quát

Windows 11 là hệ điều hành mới nhất của Microsoft, được thiết kế với nền tảng bảo mật tiên tiến nhất hiện nay. So với các phiên bản trước, Windows 11 sở hữu nhiều đặc tính bảo mật độc quyền, giúp bảo vệ hệ thống toàn diện từ phần cứng đến phần mềm.

3.2 Các đặc tính bảo mật riêng biệt

3.2.1 Security by Design & Security by Default

Security by Design: Windows 11 tuân theo nguyên tắc phát triển phần mềm an toàn (Security Development Lifecycle - SDL), trong đó bảo mật được tích hợp ngay từ giai đoạn thiết kế, thay vì là một tính năng bổ sung sau này.

Security by Default: Windows 11 mặc định kích hoạt nhiều cơ chế bảo mật quan trọng mà không yêu cầu người dùng hoặc quản trị viên phải cấu hình thêm.

Windows 11 là hệ điều hành đầu tiên yêu cầu bảo mật mặc định ngay từ khi cài đặt.Tính năng bảo mật không còn là "tùy chọn" như trên Windows 10 mà trở thành tiêu chuẩn bắt buộc.

- Yêu cầu phần cứng bảo mật bắt buộc (TPM 2.0 & UEFI Secure Boot).
- Bật mặc định Virtualization-Based Security (VBS) và Hypervisor-Protected Code Integrity (HVCI) trên tất cả các thiết bị.
- Local Security Authority Protection (LSA Protection) mặc định kích hoạt, bảo vệ danh tính khỏi tấn công giả mạo.
- Config Refresh (Windows 11 24H2) – Tự động reset lại các thiết lập bảo mật quan trọng để đảm bảo không bị chỉnh sửa trái phép.

3.2.2 Bảo mật ngay từ phần cứng & firmware

Windows 11 là hệ điều hành đầu tiên tích hợp chặt chẽ bảo mật phần cứng với phần mềm, đảm bảo thiết bị luôn ở trạng thái sạch và đáng tin cậy ngay từ khi khởi động.

Secured-core PC (SCPC) và Edge Secured-Core (ESc) dành cho thiết bị IoT là những nền tảng bảo mật cao cấp, giúp bảo vệ các hệ thống quan trọng như tài chính, chính phủ và y tế khỏi tấn công firmware.

- Chỉ Windows 11 yêu cầu Secured-core PC trên nhiều dòng thiết bị, giúp bảo vệ firmware khỏi rootkit và bootkit.
- Hỗ trợ Microsoft Pluton Security Processor, chip bảo mật chỉ có trên Windows 11, cung cấp khả năng bảo vệ phần cứng tốt hơn so với TPM rời.
- Edge Secured-Core (ESc) dành riêng cho thiết bị IoT, giúp bảo vệ các hệ thống quan trọng như y tế và chính phủ.

3.2.3 Loại bỏ mật khẩu truyền thống, tăng cường bảo vệ danh tính

Windows 11 thay thế mật khẩu bằng Passkeys, Windows Hello, và xác thực FIDO2, giúp giảm nguy cơ bị lừa đảo hoặc đánh cắp thông tin đăng nhập.

- Windows Hello: Xác thực sinh trắc học (khuôn mặt, vân tay) hoặc PIN bảo mật lưu trữ trong TPM.
- Passkeys & FIDO2: Thay thế mật khẩu bằng khóa xác thực mạnh, chống phishing.
- Credential Guard: Cách ly thông tin đăng nhập để ngăn chặn tấn công Pass-the-Hash.

3.2.4 Bảo vệ hệ điều hành bằng công nghệ ảo hóa & kiểm soát mã độc kernel

Windows 11 sử dụng bảo mật dựa trên ảo hóa (VBS) để cô lập các tiến trình bảo mật quan trọng khỏi sự can thiệp của malware.

- Virtualization-Based Security (VBS): Cách ly các tiến trình quan trọng trong một vùng bảo mật riêng biệt.
- Hypervisor-Protected Code Integrity (HVCI): Ngăn chặn mã độc kernel, chỉ cho phép chạy driver đã được ký số hợp lệ.
- LSA Protection: Bảo vệ tiến trình quản lý xác thực khỏi bị tấn công.

3.2.5 Phòng chống tấn công mạng và phần mềm độc hại theo thời gian thực

Windows 11 có hệ thống bảo vệ mạng và phần mềm độc hại thông minh, tích hợp chặt chẽ với AI và máy học để phát hiện mối đe dọa mới.

- Microsoft Defender SmartScreen: Chặn trang web độc hại và bảo vệ người dùng khỏi các cuộc tấn công phishing.
- Enhanced Phishing Protection: Cảnh báo nếu người dùng nhập mật khẩu vào trang web không an toàn.
- Microsoft Defender for Endpoint (EDR): Phát hiện, phản ứng và cô lập các mối đe dọa nâng cao.

3.3 Kết chương

Chương này đã trình bày các đặc tính bảo mật độc quyền của Windows 11, bao gồm Security by Design & Security by Default, bảo vệ từ phần cứng với Secured-core PC & Microsoft Pluton, xác thực không mật khẩu với Passkeys & Windows Hello, bảo vệ hệ điều hành bằng ảo hóa, và phòng chống tấn công mạng với Defender SmartScreen & Enhanced Phishing Protection. Những công nghệ này giúp Windows 11 đạt tiêu chuẩn bảo mật cao nhất từ trước đến nay.

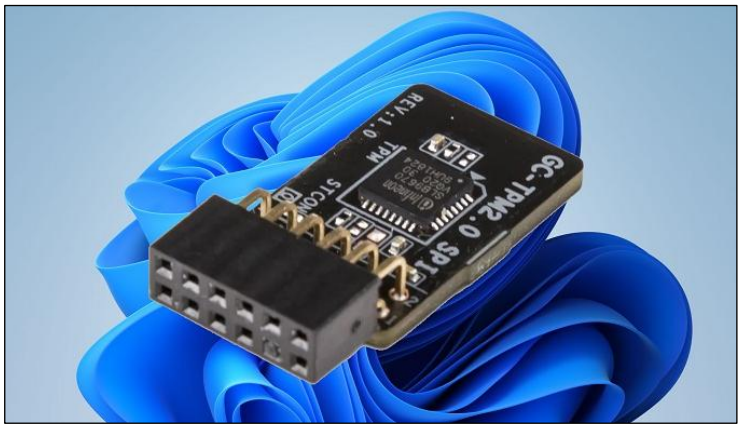
CHƯƠNG 4. CÁC THÀNH PHẦN CỦA HỆ THỐNG BẢO MẬT

4.1 Bảo mật phần cứng (Hardware Security)

4.1.1 TPM 2.0 (Trusted Platform Module 2.0)

Công nghệ Trusted Platform Module (TPM) được thiết kế để cung cấp các chức năng bảo mật dựa trên phần cứng. Chip TPM là một bộ vi xử lý nằm trên bo mạch chủ của máy tính, nó riêng biệt với CPU được thiết kế để bảo mật phần cứng thông qua các khóa mật mã tích hợp, đồng thời giao tiếp với các bộ phận còn lại của máy tính thông qua phần cứng.

Windows Hello, BitLocker, System Guard và các tính năng khác của Windows dựa vào TPM để thực hiện các chức năng như tạo khóa, lưu trữ an toàn, mã hóa, đo lường tính toàn vẹn khi khởi động và xác thực.



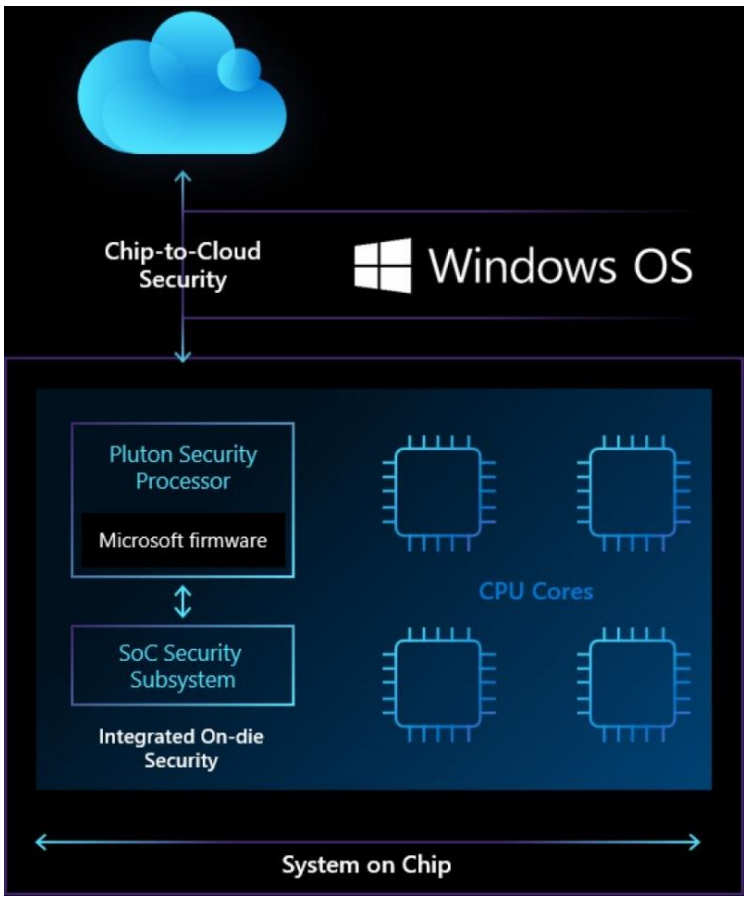
Hình 3 - Con chip TPM

Phiên bản TPM 2.0 bao gồm hỗ trợ các thuật toán mới hơn, giúp cải thiện các khả năng như hỗ trợ mật mã mạnh hơn. Một số lợi ích chính của chip bảo mật TPM 2.0:

- Hỗ trợ mã hóa ổ đĩa trên máy với công nghệ Bitlocker: Mã hóa ổ cứng, yêu cầu mật mã để truy cập, ngăn chặn truy cập trái phép.
- Mã hóa mật khẩu: Chuyển đổi mật khẩu thành dạng khó đoán, chống công cụ phá khóa.
- Chống virus & malware: Phát hiện sửa đổi dữ liệu bất thường, cảnh báo người dùng và hỗ trợ quét trong Safe Mode.

4.1.2 Microsoft Pluton

Microsoft Pluton là bộ xử lý bảo mật được tích hợp trực tiếp vào CPU, giúp giảm nguy cơ tấn công vật lý so với các TPM truyền thống nằm trên bo mạch chủ. Pluton tuân theo tiêu chuẩn TPM 2.0, hỗ trợ các tính năng bảo mật quan trọng như BitLocker, Windows Hello, và System Guard. Ngoài ra, Pluton có thể mở rộng chức năng bảo mật thông qua các bản cập nhật hệ điều hành và firmware.

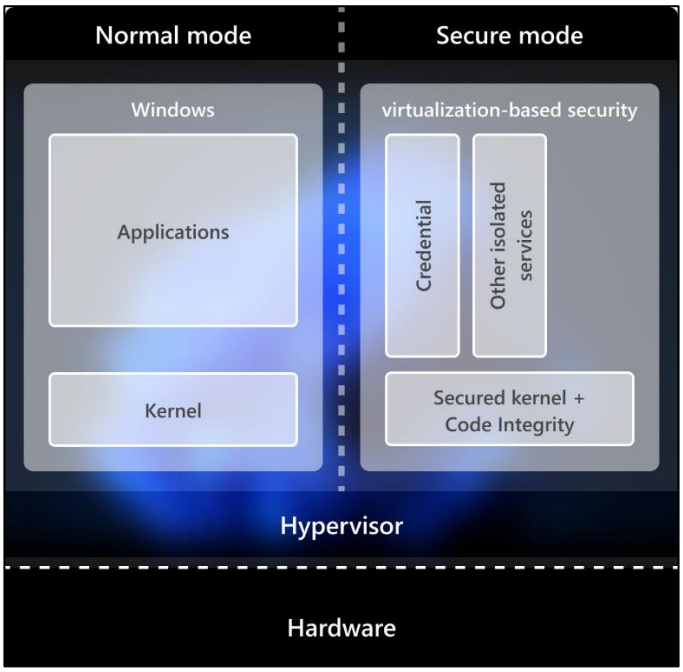


Hình 4 - Kiến trúc Microsoft Pluton

4.1.3 Virtualization-Based Security (VBS)

Bảo mật dựa trên ảo hóa (VBS) là cơ chế bảo mật sử dụng ảo hóa phần cứng để tạo một nhân bảo mật riêng biệt với hệ điều hành, giúp bảo vệ thông tin quan trọng ngay cả khi hệ điều hành bị xâm phạm.

- Cô lập tiến trình quan trọng: Bảo vệ các giải pháp bảo mật và trình quản lý thông tin xác thực khỏi phần mềm độc hại.
- Chống tấn công kernel: Nếu phần mềm độc hại kiểm soát nhân chính, phần cứng ảo hóa vẫn ngăn nó thực thi mã trái phép hoặc truy cập dữ liệu nhạy cảm.
- Hỗ trợ Hypervisor-Protected Code Integrity (HVCI) để ngăn mã độc thay đổi bộ nhớ nhân hệ điều hành.



Hình 5 - Kiến trúc bảo mật dựa trên ảo hóa (VBS)

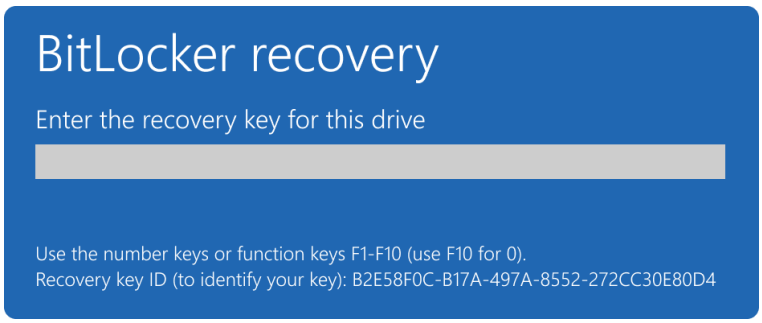
4.2 Bảo mật hệ điều hành (Operating System security)

4.2.1 Mã hóa và bảo vệ dữ liệu (Encryption and data protection)

4.2.1.1 BitLocker

BitLocker là tính năng bảo vệ dữ liệu được tích hợp trong hệ điều hành, giúp mã hóa dữ liệu để chống lại rủi ro đánh cắp hoặc lộ thông tin khi thiết bị bị mất, đánh cắp hoặc xử lý không đúng cách.

- Mã hóa mạnh mẽ: Sử dụng thuật toán AES (XTS/CBC) với khóa 128 hoặc 256-bit để mã hóa dữ liệu trên ổ đĩa.
- Lưu trữ khóa khôi phục: Khi BitLocker được bật trong quá trình thiết lập ban đầu (OOBE), mật khẩu khôi phục tự động được lưu vào tài khoản Microsoft (MSA). Người dùng cũng có thể xuất khóa khôi phục và lưu trên OneDrive hoặc Azure.
- Quản lý doanh nghiệp: Các tổ chức có thể quản lý BitLocker thông qua Group Policy hoặc Microsoft Intune để mã hóa hệ điều hành, ổ dữ liệu cố định và ổ di động (BitLocker To Go).
- Tích hợp bảo mật phần cứng: Hỗ trợ các công nghệ như TPM, UEFI Secure Boot, HSTI và Modern Standby để tăng cường an toàn dữ liệu.



Hình 6 - Yêu cầu khóa khôi phục Bitlocker

4.2.1.2 Ổ cứng tự mã hóa (Encrypted Hard Drive)

Encrypted Hard Drive là loại ổ cứng tự mã hóa dữ liệu ngay từ phần cứng, kết hợp với BitLocker để tăng cường bảo mật mà không cần phần mềm bên ngoài.

- Tích hợp BitLocker: Cung cấp mã hóa mạnh mẽ, luôn bật, khóa mã hóa không rời khỏi ổ cứng, bảo vệ ngay cả khi hệ điều hành bị tấn công.
- Hiệu suất cao, tiết kiệm tài nguyên: Mã hóa phần cứng giảm tải cho CPU, tiết kiệm năng lượng, không ảnh hưởng hiệu suất hệ thống.
- Dễ sử dụng & quản lý: Tự động mã hóa, không cần thiết lập thủ công, dễ dàng xóa dữ liệu bằng khóa mã hóa tích hợp, không cần mã hóa lại toàn bộ ổ đĩa.
- Giảm chi phí quản lý: Không cần hạ tầng mới, tận dụng hệ thống BitLocker hiện có, giúp thiết bị hoạt động hiệu quả hơn.

4.2.2 Bảo mật hệ thống (System security)

4.2.2.1 Trusted Boot

Trusted Boot là cơ chế bảo mật khởi động trên Windows 11, kết hợp với Secure Boot để ngăn chặn phần mềm độc hại và rootkit ngay từ quá trình khởi động.

- Secure Boot: Xác minh chữ ký số của firmware, bootloader và mã khởi động, ngăn chặn rootkit và malware chỉnh sửa hệ thống trước khi Windows khởi chạy.
- Trusted Boot: Tiếp tục kiểm tra tính toàn vẹn của Windows kernel, driver khởi động và phần mềm chống virus (ELAM) trước khi tải hệ điều hành. Nếu phát hiện lỗi, Windows có thể tự động sửa chữa để đảm bảo khởi động an toàn.

4.2.2.2 Windows Security

Windows Security cung cấp tổng quan nhanh về trạng thái bảo mật và sức khỏe thiết bị, giúp người dùng nhận diện vấn đề và bảo vệ hệ thống kịp thời.

- Giám sát bảo mật toàn diện: Hiển thị tình trạng chống virus, bảo vệ tường lửa, an ninh mạng, và các biện pháp bảo vệ thiết bị.
- Phát hiện và cảnh báo sớm: Giúp người dùng nhanh chóng xác định rủi ro và thực hiện hành động bảo vệ hệ thống.

4.2.3 Bảo mật mạng (Network security)

4.2.3.1 Domain Name System (DNS) Security

Windows 11 hỗ trợ DNS over HTTPS (DoH) và DNS over TLS (DoT) để mã hóa truy vấn DNS, giúp bảo vệ thiết bị khỏi các cuộc tấn công theo dõi hoặc chuyển hướng độc hại.

- Bảo mật DNS theo Zero Trust, chỉ kết nối với DNS đáng tin cậy.
- Quản lý linh hoạt: Quản trị viên IT có thể bắt buộc sử dụng DNS over HTTPS để chặn kết nối với các dịch vụ DNS không an toàn.
- Tích hợp với Windows DNS để đảm bảo tương thích và bảo mật.

4.2.3.2 Windows Firewall

Windows Firewall là tường lửa hai chiều giúp lọc và chặn lưu lượng trái phép, tăng cường bảo mật mạng.

- Giảm rủi ro tấn công mạng: Hạn chế bề mặt tấn công bằng cách đặt quy tắc dựa trên địa chỉ IP, cổng hoặc đường dẫn chương trình, giúp quản lý dễ dàng hơn.
- Bảo vệ dữ liệu nhạy cảm và tài sản trí tuệ: Tích hợp với IPSec (Internet Protocol Security) để xác thực và mã hóa kết nối mạng, bảo đảm tính toàn vẹn và bảo mật dữ liệu.
- Tối ưu hóa chi phí đầu tư: Không cần phần cứng hoặc phần mềm bổ sung, hỗ trợ tích hợp với các giải pháp bảo mật khác.

4.2.3.3 Virtual Private Networks (VPN)

VPN tạo ra một kết nối an toàn và mã hóa giữa máy tính và một máy chủ VPN. Tất cả lưu lượng truy cập internet sẽ được chuyển qua máy chủ VPN này, giúp che giấu địa chỉ IP thực và bảo vệ dữ liệu khỏi bị đánh cắp hoặc theo dõi.

Cung cấp kết nối an toàn và dễ quản lý với nhiều giao thức VPN có sẵn. Người dùng có thể kiểm soát VPN ngay trên Quick Actions của Windows 11, giúp bật/tắt và kiểm tra trạng thái nhanh chóng.

Tối ưu hóa cho các dịch vụ VPN đám mây như Azure VPN, tích hợp giao diện Windows giúp quản trị viên IT dễ dàng cấu hình và kiểm soát kết nối, đảm bảo sự nhất quán trong xác thực và quản lý truy cập từ xa.

4.2.4 Ngăn chặn virus và các mối đe dọa (Virus and threat protection)

Microsoft Defender Antivirus, SmartScreen, giảm tấn công bề mặt, bảo vệ chống xâm nhập, kiểm soát thư mục.

4.2.4.1 Microsoft Defender SmartScreen

Microsoft Defender SmartScreen bảo vệ người dùng khỏi lừa đảo trực tuyến (phishing), trang web và ứng dụng độc hại, cũng như tệp tải xuống nguy hiểm.

- Phát hiện trang web độc hại bằng cách phân tích hành vi đáng ngờ và so sánh với danh sách trang web lừa đảo đã báo cáo. Nếu trang web có rủi ro, SmartScreen sẽ cảnh báo người dùng.

- Kiểm tra ứng dụng tải xuống bằng cách đối chiếu với danh sách phần mềm độc hại đã biết. Nếu tệp tải xuống nguy hiểm hoặc không phổ biến, SmartScreen sẽ hiển thị cảnh báo.
- Bảo vệ tài khoản Microsoft, cảnh báo khi nhập thông tin vào trang web không an toàn.

4.2.4.2 Microsoft Defender Antivirus

Microsoft Defender Antivirus là giải pháp bảo vệ thế hệ mới, được tích hợp sẵn trong Windows 10 và Windows 11, cung cấp bảo vệ theo thời gian thực trước virus, phần mềm độc hại và ứng dụng không mong muốn.

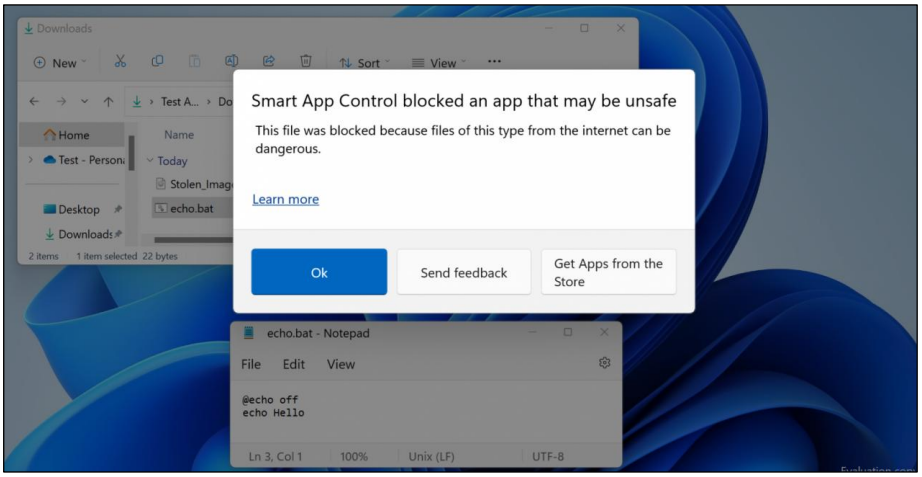
- Tự động cập nhật & giám sát liên tục để bảo vệ thiết bị khỏi các mối đe dọa mới.
- Tích hợp công nghệ AI & đám mây, giúp phát hiện nhanh chóng và ngăn chặn tấn công mạng.
- Tự động vô hiệu hóa khi cài phần mềm diệt virus khác và kích hoạt lại khi cần thiết.

4.3 Bảo mật ứng dụng (Application security)

4.3.1 Smart App Control

Smart App Control (SAC) giúp ngăn chặn phần mềm độc hại, ứng dụng không tin cậy hoặc chưa được ký số. Đây là lớp bảo mật bổ sung so với các cơ chế bảo vệ trước đây, được tích hợp trực tiếp vào hệ điều hành ở cấp độ tiến trình.

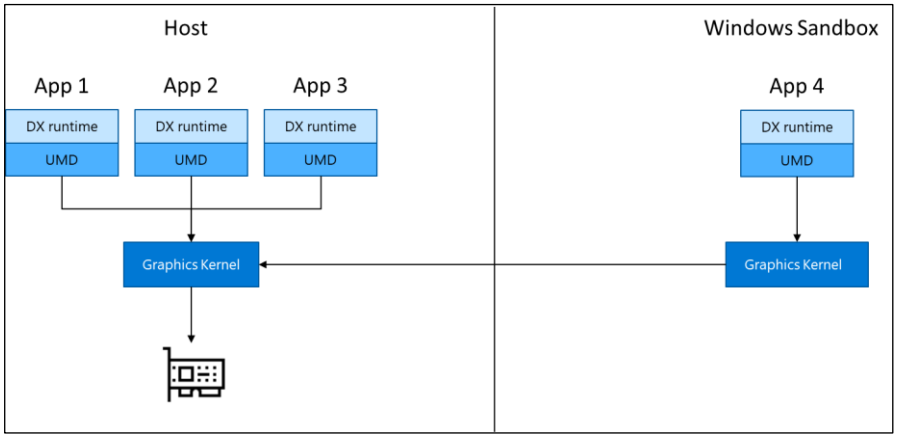
Smart App Control kế thừa công nghệ AI từ App Control for Business, giúp người dùng yên tâm rằng các ứng dụng họ sử dụng là an toàn và đáng tin cậy. Người dùng cần cập nhật Windows thường xuyên để tận dụng các cải tiến bảo mật mới nhất của Smart App Control.



Hình 7 - Smart App Control chặn tập tin không an toàn

4.3.2 Windows Sandbox

Windows Sandbox cung cấp một môi trường ảo hóa nhẹ để chạy ứng dụng Win32 không đáng tin cậy một cách an toàn. Nó sử dụng công nghệ ảo hóa phần cứng Hyper-V, đảm bảo rằng các ứng dụng chạy trong Sandbox không thể ảnh hưởng đến hệ thống chính.



Hình 8 - Kiến trúc Windows Sandbox và Host

- Khi mở Windows Sandbox, hệ thống sẽ tạo một bản sao nhẹ của Windows 11 trong môi trường ảo hóa.
- Ứng dụng chạy bên trong Sandbox không thể truy cập dữ liệu hệ thống chính.
- Khi đóng Sandbox, mọi dữ liệu và ứng dụng trong đó sẽ bị xóa hoàn toàn, đảm bảo không có phần mềm độc hại nào còn tồn tại.

4.4 Bảo mật danh tính và xác thực (Identity & Authentication Security)

4.4.1 Windows Hello

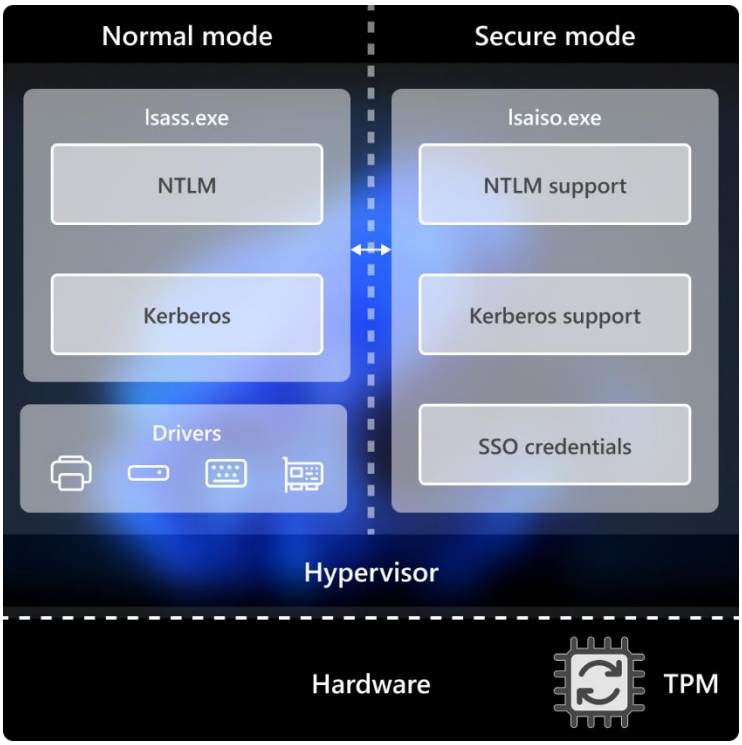
Windows Hello cung cấp xác thực sinh trắc học (khuôn mặt, vân tay) hoặc mã PIN, thay thế mật khẩu truyền thống, giảm thiểu rủi ro bị đánh cắp thông tin đăng nhập.

- Windows Hello – Đăng nhập không cần mật khẩu: Thay thế mật khẩu bằng PIN hoặc sinh trắc học, hỗ trợ FIDO2; bảo vệ thông tin đăng nhập bằng TPM, chống tấn công dò mật khẩu, phishing và giả mạo.
- Windows Hello PIN: Chỉ có thể nhập trên thiết bị, không thể truy xuất từ xa; bảo vệ bởi TPM, ngăn chặn tấn công brute-force; hỗ trợ bảo mật dựa trên ảo hóa (VBS)
- Windows Hello Biometric: Đăng nhập nhanh, an toàn bằng vân tay hoặc nhận diện khuôn mặt; hỗ trợ phần cứng đáng tin cậy, có thể vô hiệu hóa camera bên ngoài.
- Windows Hello for Business hỗ trợ xác thực không cần mật khẩu
  + Tích hợp với Microsoft Entra ID hỗ trợ đăng nhập một lần (SSO).
  + Temporary Access Pass (TAP) (mã tạm thời với bảo mật cao).
  + Xác thực đa yếu tố (MFA) với Microsoft Authenticator.

4.4.2 Credential Guard

Credential Guard sử dụng bảo mật dựa trên ảo hóa (VBS) để bảo vệ thông tin đăng nhập, giúp ngăn chặn tấn công đánh cắp thông tin xác thực. Chống tấn công đánh cắp thông tin đăng nhập, bao gồm Pass-the-Hash & Pass-the-Ticket. Cụ thể, Credential Guard sẽ cô lập các secrets đăng nhập của Windows (như hash mật khẩu NTLM, vé Kerberos...) trong

một vùng an toàn tách biệt khỏi hệ điều hành chính. Tính năng này xuất hiện từ thời Windows 10 nhưng thường tắt mặc định; còn trên Windows 11 (đặc biệt bản Enterprise) thì Microsoft đã kích hoạt sẵn nhằm giảm thiểu nguy cơ lộ lọt thông tin đăng nhập trong môi trường doanh nghiệp.



Hình 9 - Cơ chế bảo vệ thông tin đăng nhập với Credential Guard

4.5 Kết chương

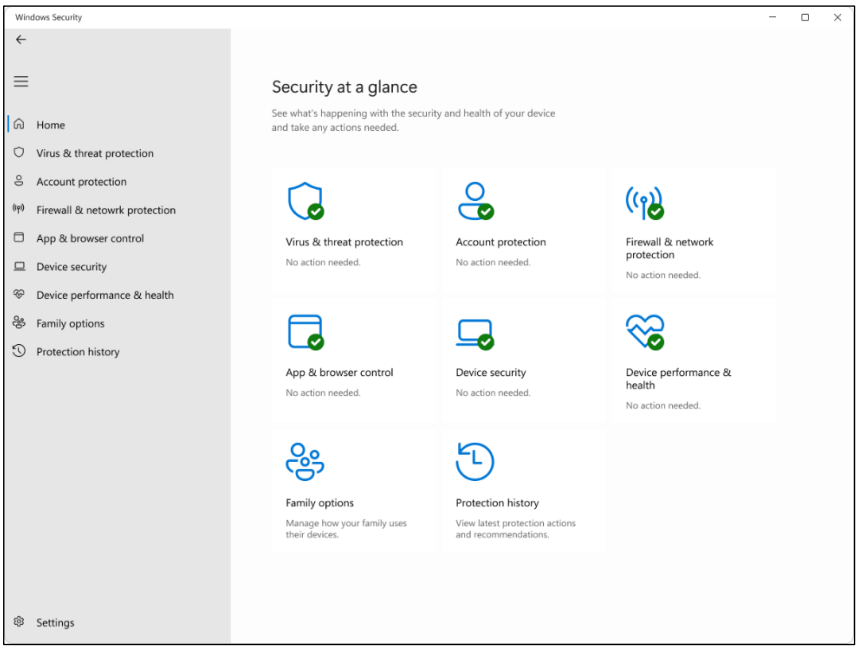
Chương này đã trình bày các thành phần quan trọng của hệ thống bảo mật Windows 11, bao gồm bảo mật phần cứng, hệ điều hành, ứng dụng và xác thực danh tính. Việc áp dụng bảo mật đa lớp giúp Windows chống lại các mối đe dọa ngày càng tinh vi.

CHƯƠNG 5. CÁC CÔNG CỤ ĐẢM BẢO AN TOÀN

5.1 Công Cụ Bảo Mật Tích Hợp

5.1.1 Windows Security

Windows Security là trung tâm quản lý bảo mật của Windows 11, cung cấp giao diện giám sát virus, tường lửa, bảo vệ ứng dụng, giúp người dùng dễ dàng kiểm soát trạng thái bảo mật của hệ thống.

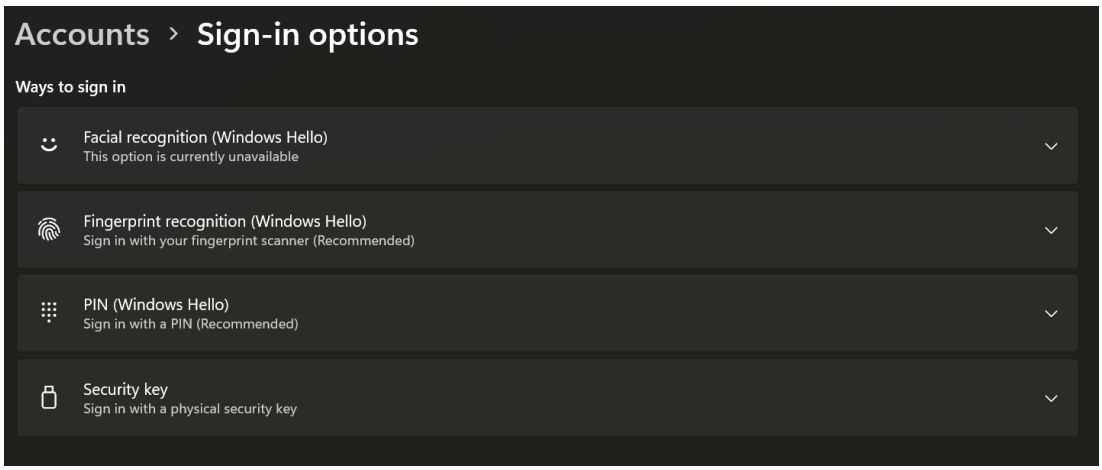


Hình 10 - Windows Security

- Ngăn chặn mối đe dọa và virus (Virus & Threat Protection): Theo dõi và ngăn chặn phần mềm độc hại, cung cấp cập nhật bảo mật kịp thời.
- Bảo vệ tài khoản (Account Protection): Quản lý quyền truy cập, xác thực danh tính an toàn qua Windows Hello, TPM 2.0.
- Bảo vệ mạng (Firewall & Network Protection): Giám sát và kiểm soát các kết nối internet, ngăn chặn truy cập không an toàn.
- Kiểm soát ứng dụng (App & Browser Control): Bảo vệ khi duyệt web và sử dụng ứng dụng, ngăn chặn nội dung độc hại qua Microsoft Defender SmartScreen.
- Bảo vệ thiết bị (Device Security): Kiểm tra lỗ hổng bảo mật, sử dụng UEFI Secure Boot, Virtualization-based Security (VBS) để ngăn mã độc xâm nhập.
- Theo dõi tình trạng hoạt động (Device Performance & Health): Cung cấp thông tin về tình trạng hệ thống, giúp duy trì hiệu suất và bảo mật thiết bị.

5.1.2 Windows Hello

Windows Hello cho phép đăng nhập không cần mật khẩu bằng sinh trắc học (vân tay, khuôn mặt) hoặc PIN an toàn, giúp chống phishing và bảo vệ tài khoản người dùng.



Hình 11 - Windows Hello trên Windows 11

5.1.3 BitLocker

BitLocker giúp mã hóa ổ đĩa hệ thống và USB, ngăn chặn truy cập trái phép nếu thiết bị bị đánh cắp, tích hợp với TPM để bảo vệ khóa mã hóa.

- Mã hóa Thiết bị, được thiết kế để sử dụng đơn giản và thường được bật tự động
- Mật mã hóa Ổ BitLocker , được thiết kế cho các trường hợp nâng cao và cho phép người dùng mã hóa ổ đĩa theo cách thủ công

Ngoài ra, còn có Windows Defender SmartScreen (ngăn chặn phishing), Windows Firewall (tường lửa bảo vệ hệ thống), và Secure Boot (bảo vệ quá trình khởi động khỏi rootkit/malware).

5.2 Công Cụ Bảo Mật Nâng Cao

5.2.1 Microsoft Defender for Endpoint

Microsoft Defender for Endpoint là giải pháp bảo vệ đầu cuối (EDR) giúp phát hiện và phản hồi mối đe dọa nâng cao, chống lại ransomware, malware, và tích hợp với Microsoft Intune để quản lý bảo mật từ xa.

- Tích hợp cảm biến hành vi trong Windows, thu thập dữ liệu và phân tích trên đám mây bảo mật.
- Tình báo bảo mật mạnh mẽ, xử lý 43 nghìn tỷ tín hiệu/ngày, giúp chặn mối đe dọa danh tính và email.
- Hệ thống hỗ trợ cô lập thiết bị, chặn tệp độc hại, điều tra & khắc phục sự cố từ xa, giúp tăng tốc phản ứng trước các cuộc tấn công.

5.2.2 Virtualization-based Security (VBS) & Hypervisor-Protected Code Integrity (HVCI)

VBS (Virtualization-based Security) tạo một vùng bộ nhớ ảo hóa tách biệt để bảo vệ các thông tin nhạy cảm như credential hashes, giúp chống lại các cuộc tấn công Pass-the-Hash, Pass-the-Ticket. Ngay cả khi hệ điều hành chính bị xâm nhập, malware cũng không thể truy cập vào dữ liệu bảo mật này.

HVCI (Hypervisor-Protected Code Integrity) sử dụng công nghệ ảo hóa để đảm bảo chỉ các đoạn mã hệ thống đã được xác thực mới có thể chạy trong không gian kernel. Điều này giúp ngăn chặn các cuộc tấn công như injection mã độc vào kernel, bảo vệ tính toàn vẹn của hệ điều hành.

Kết hợp với nhau, VBS và HVCI giúp gia cố lớp bảo mật của Windows 11, bảo vệ hệ thống khỏi bootkit, rootkit và các phương pháp tấn công nhằm vào kernel

5.2.3 Windows Sandbox

Windows Sandbox cung cấp môi trường ảo hóa "dùng một lần", giúp thử nghiệm phần mềm không tin cậy mà không ảnh hưởng đến hệ thống chính.

Ngoài ra, có các công cụ như Credential Guard (bảo vệ danh tính), Smart App Control (AI kiểm soát ứng dụng), Secure Boot với Measured Boot (xác minh quá trình khởi động), và Application Control (quản lý phần mềm chạy trên hệ thống).

5.3 Kết chương

Chương này đã đưa ra một số công cụ đảm bảo an toàn bảo mật cho hệ điều hành Windows11. Windows 11 mang đến một hệ thống bảo mật toàn diện với nhiều công cụ tiên tiến. Việc chuyển đổi sang Windows 11 không chỉ giúp tận dụng các tính năng bảo mật mới nhất mà còn đảm bảo thiết bị luôn được cập nhật và bảo vệ khỏi các mối đe dọa an ninh mạng.

CHƯƠNG 6. DEMO & ĐÁNH GIÁ

6.1 Mô tả mô hình demo

6.1.1 Mục tiêu

- Kiểm tra khả năng bảo vệ của Microsoft Defender Antivirus trước mối đe dọa phổ biến.
- Đánh giá hiệu suất hệ thống khi sử dụng Defender Antivirus.
- Kiểm tra khả năng quản lý và giám sát bảo mật qua Windows Security.

6.1.2 Cấu hình hệ thống thử nghiệm

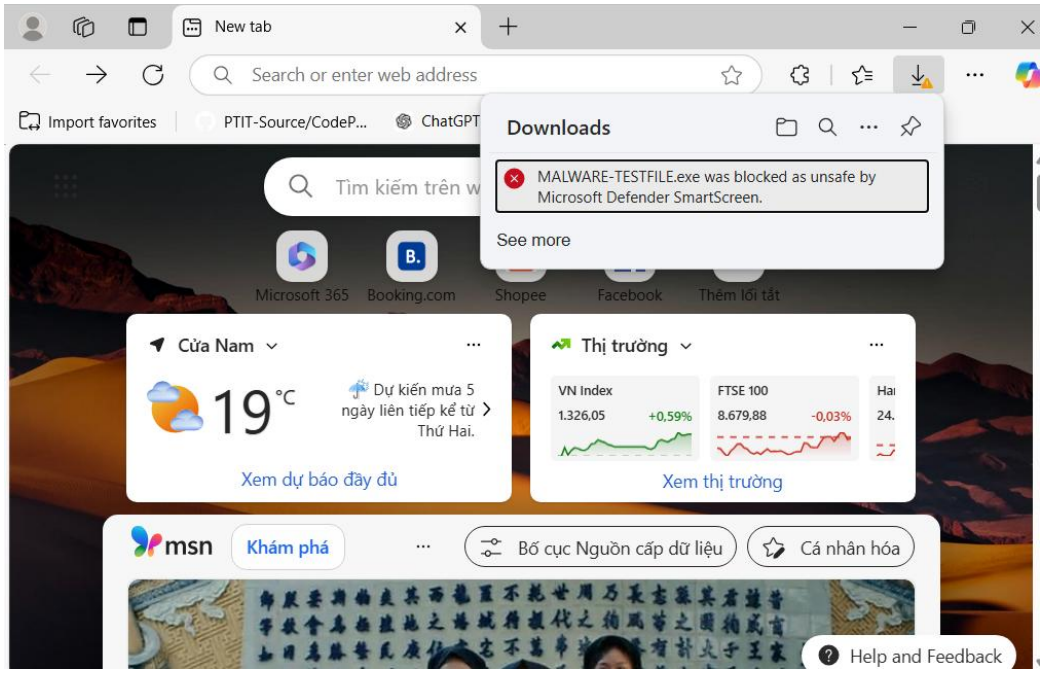
- Hệ điều hành: Windows 11 Pro 23H2 (đã cập nhật bản vá bảo mật mới nhất).
- Phần cứng: Máy tính hoặc máy ảo với:
  - CPU: Intel Core i5 hoặc AMD Ryzen 5 trở lên.
  - RAM: 8GB hoặc cao hơn.
  - Ổ cứng: SSD 256GB trở lên.
  - TPM 2.0, Secure Boot được bật.
- Công cụ kiểm thử:
  - EICAR Test File (file giả lập virus an toàn, giúp kiểm tra phản ứng của phần mềm chống virus).

6.1.3 Kịch bản: Kiểm tra bảo vệ thời gian thực (Real-time Protection)

- Mục tiêu: Xác minh Microsoft Defender Antivirus có thể tự động phát hiện và chặn virus ngay khi tải xuống hoặc sao chép vào hệ thống.
- Các bước thực hiện:

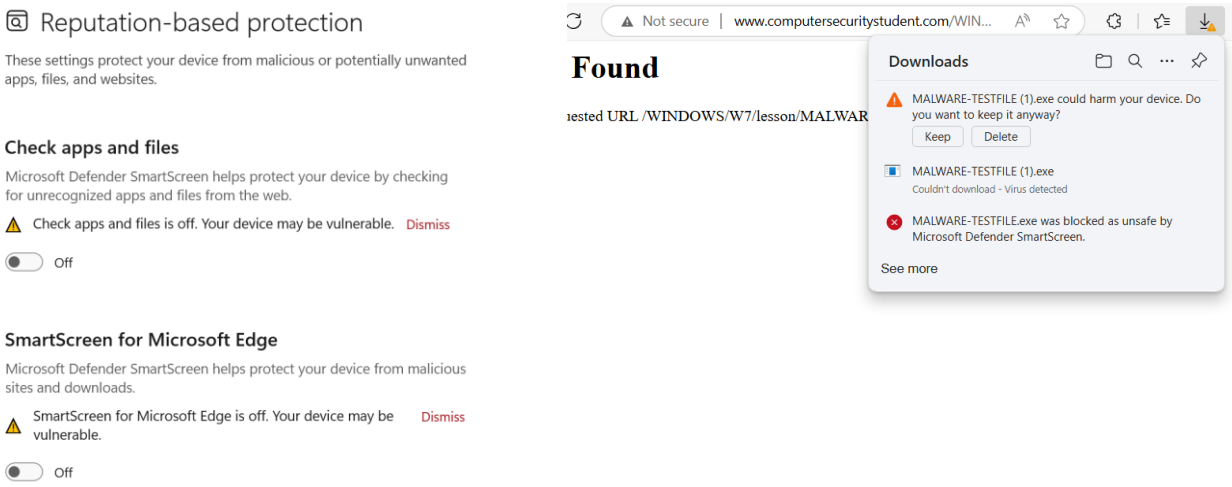
  Dùng Web browser tải file test mã độc từ đường link:

  http://www.computersecuritystudent.com/WINDOWS/W7/lesson7/MALWARE-TESTFILE.exe



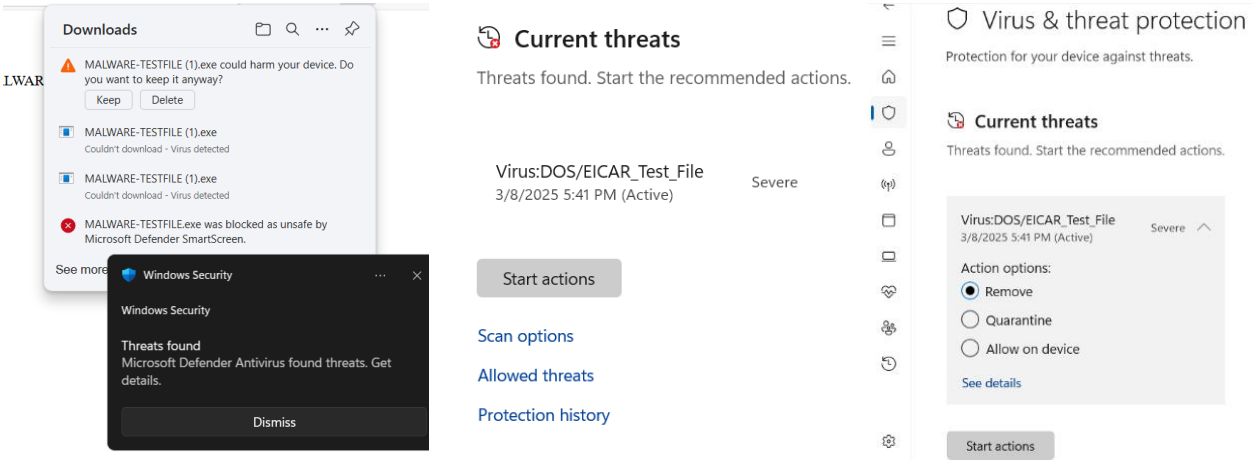
Hình 12 - Tiến hành tải file mã độc không thành công do bị chặn bởi SmartScreen

Tiến hành tắt SmartScreen và cố gắng tải file mã độc về



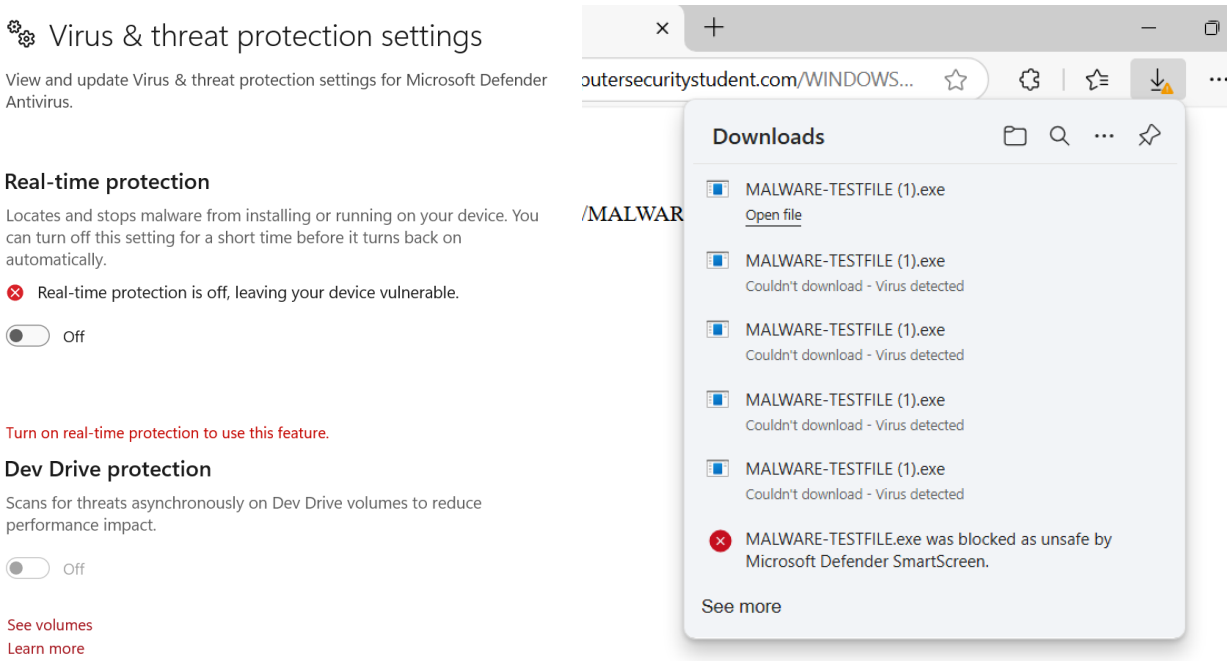
Hình 13 – Cố gắng tải file mã độc sau khi tắt SmartScreen

Kiểm tra thông báo của Windows Security.



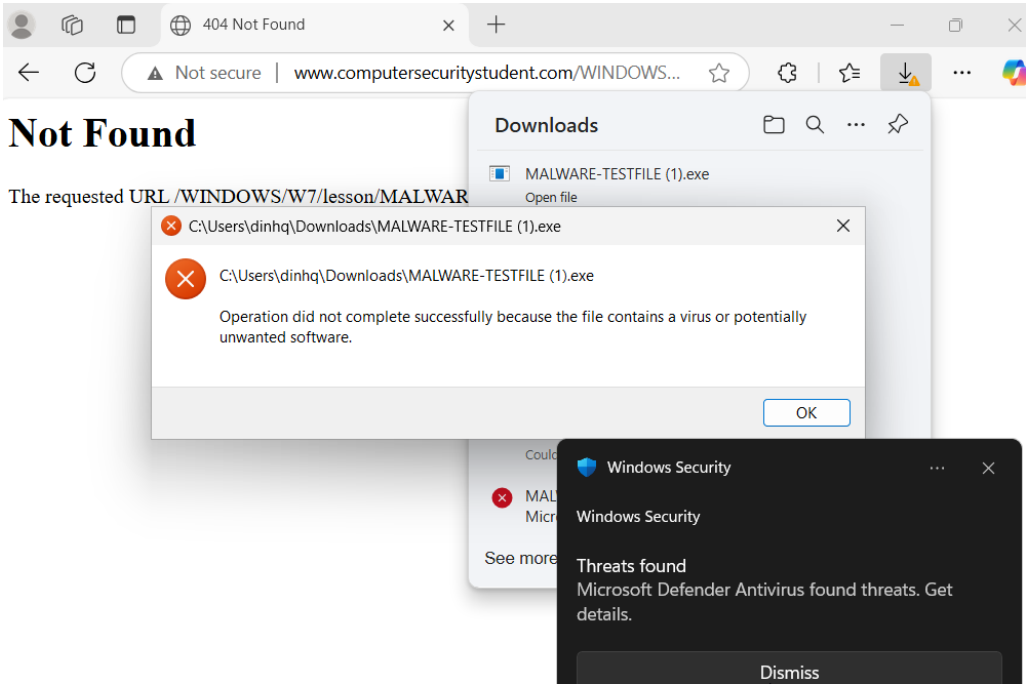
Hình 14 - Thông báo của Windows Security khi muốn tải file mã độc

Nếu tắt luôn hệ thống bảo vệ thời gian thực đi, thành công tải mã độc về máy.



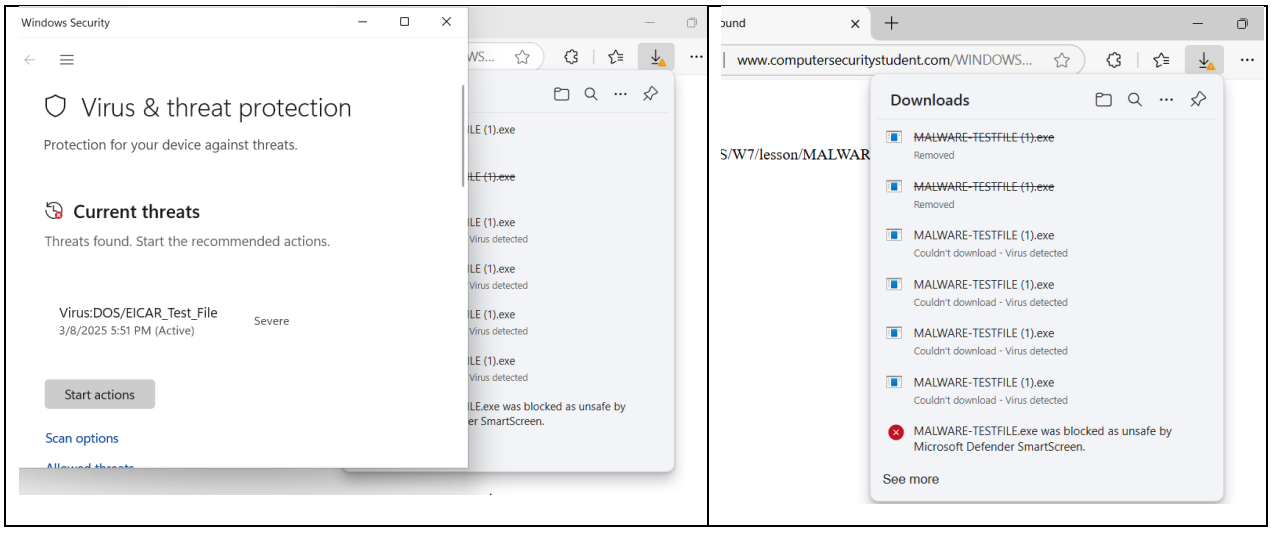
Hình 15 - Tắt Real-time protection và thành công tải file mã độc

Bật lại hệ thống bảo vệ thời gian thực Real-time protection sau khi đã tải file mã độc về, Windows Sercurity ngay lập tức hiển thị cảnh báo rằng Microsoft Defender Antivirus đã tìm thấy mối đe dọa.



Hình 16 - Windows Security hiển thị thông báo khi phát hiện file mã độc trong máy

Click Start actions, file mã độc sẽ bị xóa khỏi máy. Thậm chí không cần người dùng bấm xóa thì file cũng tự động bị xóa.



Hình 17 - Microsoft Defender Antivirus cách ly và tự động xóa file mã độc

6.2 Đánh giá

Hiệu suất hệ thống: Defender Antivirus hoạt động mượt mà, không làm giảm tốc độ xử lý của hệ thống. Tính năng bảo vệ thời gian thực tự động phát hiện, cách ly và xóa file mã độc ngay khi phát hiện.

Quản lý và giám sát bảo mật: Windows Security cung cấp giao diện trực quan và các cảnh báo kịp thời, giúp người dùng dễ dàng theo dõi và xử lý các mối đe dọa.

6.3 Kết chương

Chương này đã demo quá trình sử dụng Microsoft Defender Antivirus và Windows Sercurity trong Windows 11 để kiểm tra khả năng bảo vệ hệ thống trước mối đe dọa phổ biến. Kết quả chứng minh đây là giải pháp bảo mật ổn định và hiệu quả mà không làm ảnh hưởng đến hiệu năng hệ thống.

KẾT LUẬN

Sau quá trình nghiên cứu, nhóm đã làm rõ các yếu tố quan trọng của kiến trúc bảo mật Windows 11. Với cách tiếp cận bảo mật đa lớp từ phần cứng đến phần mềm, hệ điều hành này giúp giảm thiểu rủi ro từ các cuộc tấn công mạng, những mối đe dọa phổ biến. Các cơ chế như Zero Trust, Chip-to-Cloud, TPM 2.0, Windows Hello và Microsoft Defender giúp nâng cao khả năng phòng vệ và đảm bảo an toàn dữ liệu cho người dùng.

Windows 11 không chỉ cải thiện trải nghiệm người dùng mà còn đặt nền móng vững chắc cho một môi trường số an toàn hơn. Trong tương lai, Microsoft có thể tiếp tục nâng cấp và bổ sung các tính năng bảo mật mới để đối phó với các mối đe dọa an ninh ngày càng tinh vi.

Hướng phát triển

Đề tài này có thể được mở rộng theo các hướng sau:

- Nâng cao bảo mật Windows 11 trong môi trường doanh nghiệp: Tăng cường quản lý thiết bị, kiểm soát truy cập và bảo vệ dữ liệu doanh nghiệp.
- So sánh bảo mật Windows 11 với các hệ điều hành khác: Đánh giá mức độ an toàn của Windows 11 so với macOS và Linux trong các tiêu chí như mã hóa dữ liệu, bảo mật danh tính và phòng chống mã độc.

TÀI LIỆU THAM KHẢO

[1] Windows 11 Security Book. https://learn.microsoft.com/en-us/windows/security/book/

[2] Microsoft. *Secure Future Initiative*. https://www.microsoft.com/trust-center/security/secure-future-initiative

[3] Windows Security Team. *Windows 11 Security Overview*. https://learn.microsoft.com/en-us/windows/security/book/

[4] Microsoft Defender Documentation. *Endpoint Security Features*. https://learn.microsoft.com/en-us/defender-endpoint/

[5] NIST. *Guide to Secure Operating Systems*. National Institute of Standards and Technology, 2024.